

Dépannage de l'erreur d'alarme ISE “ ; Profiler SNMP Request Failure : Serveur= Adresse NAD= Message d'erreur=Délai de la demande dépassé” ;

Table des matières

[Problème](#)

[Environnement](#)

[Résolution](#)

[Étape 1: Identifiez le NAD affecté.](#)

[Étape 2: Assurez-vous que le protocole SNMP est exécuté sur le client NAD du périphérique d'accès réseau concerné](#)

[Étape 3: Assurez-vous que la version SNMP et la chaîne de communauté SNMP ou le mot de passe d'authentification/de confidentialité SNMP correspondent, sur le NAD et dans ISE](#)

[Étape 4: Valider l'accessibilité et les ports UDP requis \(161,162\) entre le PSN ISE et le client NAD](#)

[Motif](#)

[Autres informations utiles](#)

- [Problème](#)
 - [Environnement](#)
 - [Résolution](#)
 - [Étape 1: Identifiez le NAD affecté.](#)
 - [Étape 2: Assurez-vous que le protocole SNMP est exécuté sur le client NAD du périphérique d'accès réseau concerné](#)
 - [Étape 3: Assurez-vous que la version SNMP et la chaîne de communauté SNMP ou le mot de passe d'authentification/de confidentialité SNMP correspondent, sur le NAD et dans ISE](#)
 - [Étape 4: Valider l'accessibilité et les ports UDP requis \(161,162\) entre le PSN ISE et le client NAD](#)
 - [Motif](#)
 - [Autres informations utiles](#)
-

Problème

Lors de l'examen des alarmes dans ISE, vous voyez cette erreur de profileur SNMP :

“Profiler SNMP Request Failure: Server= <NAD DEVICE Name> NAD Address=<x.x.x.x> Error Message=Request t

Environnement

- Cisco Identity Services Engine (ISE) versions 3.0.0 et ultérieures
- Service de profilage ISE activé
- Périphériques d'accès réseau (NAD) configurés pour la communication SNMP

Résolution

Étape 1: Identifiez le NAD affecté.

1. Accédez à Tableau de bord > Alarmes
2. Vérifiez les détails de l'alarme et notez le nom ou l'adresse IP du périphérique NAD concerné.
3. Vous pouvez identifier l'adresse IP du client NAD spécifique en référençant le champ « Adresse NAD » dans le message d'erreur « Profiler SNMP Request Failure ».

Étape 2: Assurez-vous que le protocole SNMP est exécuté sur le client NAD du périphérique d'accès réseau concerné

Connectez-vous à l'interface de ligne de commande du client NAD et exécutez cette commande pour vérifier si la fonction SNMP est activée.

```
show running-config | include snmp
```

Exemple de protocole SNMP v3 :

```
Switch#show running-config | include snmp
ip access-list standard snmp-access
snmp-server group my-snmp-group v3 priv read admin-view access snmp-access
snmp-server view admin-view iso included
```

Exemple de protocole SNMP v2c :

```
snmp-server community public R0
snmp-server community private RW
snmp-server host 192.168.1.100 version 2c public
```

Étape 3: Assurez-vous que la version SNMP et la chaîne de communauté SNMP ou le mot de passe d'authentification/de confidentialité SNMP correspondent, sur le NAD et dans ISE

Validez votre configuration SNMP v2c en procédant comme suit :

1. Connectez-vous à l'interface de ligne de commande du client NAD et exécutez la commande « show snmp community ».

Sortie du commutateur :

```
Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile          active
```

2. Sur ISE : Accédez à Administration > Network Resources > Network Devices.
3. Modifiez l'entrée NAD identifiée pour vous assurer que la chaîne de communauté SNMP et la version SNMP correspondent au résultat de « show snmp community ».

ISE SNMP v2c :

☒ SNMP Settings

SNMP Version

2c

▼

SNMP RO Community

public

Hide

SNMP Username

Security Level

▼

Auth Protocol

▼

Auth Password

Show

Privacy Protocol

▼

Privacy Password

Show

Polling Interval

28,800

seconds(Valid Range 600 to 86400 or zero)

☒ Link Trap Query

☒ MAC Trap Query

Originating Policy Services Node

Auto

▼

Le commutateur masque les mots de passe d'authentification/confidentialité SNMP v3. Pour vous assurer que ces informations d'identification restent correctes, entrez-les à nouveau en procédant comme suit :

1. Connectez-vous à l'interface ISE.
2. Accédez à Administration > Network Resources > Network Devices.
3. Modifiez l'entrée NAD identifiée et accédez à SNMP Settings. En cliquant sur « Afficher » sur le mot de passe d'authentification et le mot de passe de confidentialité. Vous pouvez révéler le mot de passe correspondant.

☒ **SNMP Settings**

SNMP Version	3	▼
SNMP RO Community		Show
SNMP Username	test	
Security Level	Priv	▼
Auth Protocol	SHA	▼
Auth Password	test@123	Hide
Privacy Protocol	AES128	▼
Privacy Password	test@123	Hide
Polling Interval	28,800	seconds(Valid Range 600 to 86400 or zero)
☒ Link Trap Query		
☒ MAC Trap Query		
Originating Policy Services Node	Auto	▼

4. Connectez-vous à l'interface CLI du commutateur.

- Exécutez la commande configure terminal.
- Ensuite, exécutez cette commande pour mettre à jour les informations d'identification SNMP v3 sur le commutateur.

Commande Switch :

```
snmp-server user <username> <groupname> v3 auth sha <auth-password> priv aes 128 <priv-password>
```

Exemple :

```
snmp-server user test snmpgroup v3 auth sha test@123 priv aes 128 test@123
```

Étape 4: Valider l'accessibilité et les ports UDP requis (161,162) entre le PSN ISE et le client NAD

1. Effectuez un test ping du noeud PSN activé par le profileur vers le client NAD.
2. Exécutez un test ping à partir du client NAD vers le noeud PSN.
3. Vérifiez que les ports 161 et 162 sont ouverts entre le noeud PSN et NAD.
 - Testez l'utilisation de Telnet à partir du client NAD vers le noeud activé par le profileur pour confirmer que les ports 161 et 162 sont ouverts.

```
telnet <ISE IP-address> 161  
telnet <ISE IP-address> 162
```

Motif

L'alarme Échec de la requête SNMP se produit lorsque ISE ne parvient pas à interroger correctement le périphérique d'accès réseau. Ceci est généralement dû à des incohérences de configuration concernant les chaînes de communauté SNMP, les versions ou les identifiants v3 entre les deux périphériques. En outre, les problèmes réseau tels que les pare-feu bloquant les ports UDP 161 ou 162 ou les configurations de serveur SNMP manquantes sur le NAD empêchent souvent une communication réussie.

Autres informations utiles

[Autoriser les ports ISE et les noms de domaine complets requis sur le réseau](#)

[Guide de conception de profilage ISE](#)

[Configurer les chaînes communautaires du protocole SNMP](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.